UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/757,872	01/10/2001	John S. Flowers	22192-06893	8233

23910 7590 08/02/2004

FLIESLER MEYER, LLP
FOUR EMBARCADERO CENTER
SUITE 400
SAN FRANCISCO, CA 94111

EXAMINER	
TRAN, ELLEN C	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 08/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/757,872	FLOWERS ET AL.	
	Examiner	Art Unit	
	Ellen C Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 January 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3, 5-8*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: original application filed 10 January 2001 with acknowledgement of a continuing date of 10 January 2000.

2. Claims 1-29 are currently pending in this application. Claims 1, 8, 11, 13, 17, 18, 21, 24, 25, and 27 are independent claims.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

4. Claims 1-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Jerger et al. U.S. Patent No. 6,473,800 (hereinafter '800).

As to independent claim 1, "A method for use in analyzing network security, comprising: constructing query-based rules to be used to identify network conditions" is taught in '800 col. 3, lines 5-24.

As to dependent claim 2, "wherein network conditions include vulnerability conditions and intrusion conditions" is shown in '800 col. 3, lines 5-24.

As to dependent claim 3, "wherein the step of constricting query-based rules includes constructing query-based rules from a set of lexical elements that includes a set of templates" is disclosed in '800 col. 16, lines 26-56.

As to dependent claim 4 "wherein the templates are divided into two classes comprising template types and template actions" is taught in '800 col. 14, lines 49-67.

As to dependent claim 5, "wherein the step of constructing query based rules includes constructing query-based rules from a set of lexical elements that includes a set of statements, a set of templates, and a set of reserved words" is shown in '800 col. 16, line 57 through col. 17, line 6.

As to dependent claim 6, "wherein: network conditions include vulnerability conditions and intrusion conditions; the set of statements includes SET and SELECT; the set of reserved words includes AND, TO, and WHERE; and the set of templates includes: for identifying network vulnerability conditions: Operating System, Host, Protocol, Application, Vulnerability, Port, Execute, ExecuteHex, Contains, and ContainsHex; for identifying network intrusion conditions: Operating System, Protocol, Application, Port, Length, Offset, Threshold, Contains, ContainsHex, Flags, FragmentID, IcmpType, IcmpCode, PayloadSize, and TimeToLive" is disclosed in '800 col. 21, line 31-55 and col. 26, line 24 through col. 27, line 40.

As to dependent claim 7, "wherein the step of constructing query-based rules includes associating each rule with an operating system" is taught in '800 col. 21, lines 31-55 and col. 26, line 24 through col. 27, line 40.

As to independent claim 8, A method for use in analyzing network security, comprising: constructing files to be used to identify network conditions, including vulnerability conditions and intrusion conditions" is disclosed in '800 col. 3, lines 5-24;

"from a set of lexical elements that include a set of templates, where each rule for identifying a vulnerability condition is associated with an operating system" is shown in '800 col. 21, lines 31-55 and col. 26, line 24 through col. 27, line 40.

As to dependent claims 9 and 10, these claims are substantially similar to claims 5 and 4; therefore they are rejected along the same rationale.

As to independent claim 11, "A method for use in analyzing network security, comprising: constructing a set of rules to be used to identify vulnerability conditions and intrusion conditions from a set of lexical elements that include a set of templates" is disclosed in '800 col. 3, lines 5-24;

"where each rule for identifying a vulnerability condition is associated with an operating system; and wherein the set of templates includes: for identifying network vulnerability conditions: Host, Protocol, Application, Vulnerability, Port, Execute, ExecuteHex, Contains, and ContainsHex; for identifying network intrusion conditions: Protocol, Application, Port, Length, Offset, Threshold, Contains, ContainsHex, Flags, FragmentID, IcmpType, IcmpCode, PayloadSize, and TimeToLive" is taught in '800 col. 21, lines 31-55 and col. 26, line 24 through col. 27, line 40.

As to dependent claims 12, 13, and 14, these claims contain subject matter that is substantially similar to claims 1-6; therefore they are rejected along the same rationale.

As to dependent claim 15, "wherein: the rule constructor includes a graphical user interface to receive information from a user constructing a rule; and the rule, once constructed, is stored in a rule database" is taught in '800 col. 14, lines 33-48.

As to dependent claim 16, this claim contains subject matter that is substantially similar to claim 7; therefore it is rejected along the same rationale.

As to independent claim 17, this claim is directed to the system of the method in claims 1 and 2, therefore it is rejected along the same rationale.

As to independent claim 18, this claim is directed to the system of the method in claims 1-3; therefore it is rejected along the same rationale.

As to dependent claims 19-23, these claims contain subject matter that is substantially similar to claims 5-9; therefore they are rejected along the same rationale.

As to independent claim 24, "A system for use in network security, comprising: a rule constructor that allows a user to construct rules based on specified lexical elements, where the rules are to be used to identify intrusion conditions in a network" is taught in '800 col. 3, lines 5-24;

"a database for storing the rules" is shown in '800 col. 14, lines 33-48.;

"and an intrusion detector designed to monitor network traffic and to check that network traffic against the stored rules to determine if an intrusion condition exists on the network, the intrusion detector further designed to notify a user of the presence of an intrusion condition, but only if the intrusion condition is applicable to the network" is disclosed in col. 14, lines 49-67.

As to independent claim 25, this claim is directed to the system of the method in claim 11; therefore it is rejected along the same rationale.

As to independent claim 27, this claim is directed to the computer readable medium of the method in claim 11; therefore it is rejected along the same rationale.

As to dependent claim 26, 28, and 29, these claim contain subject matter that is substantially similar to claims 12 and 4; therefore they are rejected along the same rationale.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (703) 305-8917. The examiner can normally be reached on 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5484.

Ellen. Tran
Patent Examiner
Technology Center 2134
23 July, 2004

Andrew Caldwell
Andrew Caldwell